IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

Richard Dusterhoft, *on behalf of himself and all others similarly situated*, Plaintiff, v. OneTouchPoint, Inc., Defendant.	Case No. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Richard Dusterhoft ("Plaintiff") brings this Class Action Complaint against OneTouchPoint, Inc. ("Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsel's investigations, and upon information and belief as to all other matters, as follows:

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information including, but not limited to, first and last name, address, accounts receivable balance and information regarding payments made to your account, and Social Security number (collectively, "Private Information" or "PII").

2. Defendant provides printing and mailing services for client companies within the United States. For business purposes, Defendant received the information of individuals from customer organizations which Defendant utilized to conduct mailings on behalf of their customers.[1]

[1]*Data Breach Notifications*, OFF. ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/0a2e4b99-8e95-4860-b05f62c239a13993.shtml (last visited August 2, 2022).

3. On April 28, 2022, Defendant discovered encrypted files on certain computer systems. Defendant immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to the affected systems beginning on April 27, 2022 [2] (the "Data Breach").

4. Defendant later determined that the impacted systems contained information related to individuals provided by their customers.

5. Defendant reviewed the data that was obtained in the Data Breach and Defendant confirmed that the data contained names, member IDs, and information that may have been provided during a health assessment (hereinafter referred to as "Private Information.").

6. Despite learning of the Data Breach in April 2022, Defendant did not begin notifying Plaintiff and Class Members until on or around July 27, 2022. Defendant delayed in sending notice of the Data Breach even though Defendant was well aware of the need to move quickly in responding to Data breach events.

7. As a result of the Data Breach, Plaintiff and over one million Class Members suffered ascertainable losses in the form of losing the benefit of their bargain, incurring out-of-pocket expenses, and the value of their time reasonably invested to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

8. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant

[2] *Notice of Data Security Event*, ONETOUCHPOINT, https://1touchpoint.com/notice-of-data-event (last visited August 2, 2022).

admits that the unencrypted Private Information impacted during the Data Breach included names, member IDs, and information that may have been provided during a health assessment.

9. The exposed Private Information of Plaintiff and Class Members can—and likely will—be sold on the dark web. Hackers can attempt to sell the unencrypted, unredacted Private Information to criminals. Plaintiff and Class Members now face a lifetime risk of identity theft.

10. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions, as well as the failure to protect the Private Information of Plaintiff and Class Members. In addition to Defendant's failure to prevent the Data Breach, Defendant waited several months after discovering the breach to report it to the appropriate government agencies and affected individuals.

11. As a result of this delayed response, Plaintiff and Class Members had no idea their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax

fraud, and/or unauthorized use of their Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and substantially increased risk to their Private Information which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As the result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

PARTIES

15. Plaintiff Richard Dusterhoft is a Citizen of Minnesota residing in Alexandria, Minnesota.

16. Defendant OneTouchPoint, Inc. is a corporation organized under the laws of Wisconsin and its headquarters and principal place of business is located at 1225 Walnut Ridge Dr., Hartland, WI 53029-8300.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

18. This Court has personal jurisdiction over Defendant because its principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

19. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

20. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their Private Information which includes information that is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiff and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

22. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties.

23. On information and belief, Defendant maintains the Private Information of Plaintiff and Class Members, including, but not limited to: (1) name; (2) member ID; and (3) information that may have been provided during a health assessment.

24. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

25. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information.

26. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[3]

Defendant Acquires, Collects, and Stores the Private Information of Plaintiff and Class Members

27. Defendant acquired, collected, and stored the Private Information of Plaintiff and Class Members.

28. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

[3]*See How to Protect Your Networks from RANSOMWARE*, FBI at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

29. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing Private Information and Preventing Breaches

30. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

31. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

32. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

33. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[4] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

[4] 17 C.F.R. § 248.201 (2013).

license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[5]

34. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Private Information

35. The Private Information of individuals remains highly valuable to criminals, as evidenced by the prices criminals pay to obtain such information through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[6] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[7] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[8]

36. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number and name.

37. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

---

[5] *Id*.

[6] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGIT. TRENDS, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[7] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[8] *In the Dark*, VPNOVERVIEW, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

personally identifiable information and Social Security numbers are worth more than 10x on the black market."[9]

38. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

39. The fraudulent activity resulting from the Data Breach may not come to light for years.

40. Theft of health information is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

41. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed Private Information to adjust their insureds' medical insurance premiums.

42. According to account monitoring company LogDog, medical data, such as Private Information, sells for $50 and up on the Dark Web.[10]

43. Moreover, there may be a time lag between when a harm occurs versus when the harm is discovered, and also between when Private Information is stolen and when it is used.

[9] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[10] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021).

According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

44. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Member, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

45. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

46. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially millions of individuals' detailed, personal information and, thus, the Defendant should have been on notice of the significant number of individuals who would be harmed by exposure of unencrypted data.

47. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

[11] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Aug. 23, 2021).

48. As a condition of providing its services, processing medical claims, sending bills, and/or providing collection services for treatment, Defendant requires that its customers entrust it with Private Information.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

50. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

51. Plaintiff and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their Private Information confidential and securely maintained, to use such Private Information solely for business and health care purposes, and to prevent the unauthorized disclosures of the Private Information.

Defendant failed to properly protect Plaintiff's and Class Members' Private Information

52. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[12]

53. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

[12] *Id.* at 3–4.

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[13]

54. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

[13] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001 (last accessed Aug. 23, 2021).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[14]

55. Given that Defendant was storing the Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

[14] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last accessed Aug. 23, 2021).

56. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiff and Class Members.

57. As the result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

58. Defendant sent Plaintiff and Class Members a Notice of Data Breach Letter on or around July 27, 2022. The Notice of Data Breach Letter informed Plaintiff and Class Members that:

> **What happened?** On April 28, 2022, [Defendant] discovered encrypted files on certain computer systems. [Defendant] immediately launched an investigation an investigation, with assistance of third-party forensics specialists, to determine the nature and scope of activity. Our investigation determined that there was unauthorized access to certain of our servers beginning on April 27, 202. Through the investigation, [Defendant] learned that [Defendant] would be unable to determine what specific files the unauthorized actor viewed within our network. [Defendant] provided a summary of [Defendant's] investigation to our business customers beginning on June 3, 2022. [Defendant] later determined that the impacted systems contained certain information related to you. While [Defendant] [was] unable to say definitively if your information accessed by the unauthorized actor, [Defendant] are notifying you of the event in the abundance of caution. [Defendant] has seen no evidence of misuse of any information related to this incident.
>
> **What Information was Involved?** [Defendant] determined that the following information related to you was present on the impacted [Defendant] servers: your name, member ID, and information that you may have provided during your health assessment…

59. Defendant admitted that Private Information potentially impacted in the Data Breach included names, member IDs, and information that you may have provided during your health assessment.

60. Plaintiff's Notice of Data Breach Letter stated that the Data Breach included his name, member ID, and information that Plaintiff may have provided during the health assessment.

61. Because Defendant failed to properly protect safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access Defendant's network, and access Plaintiff's and Class Members' Private Information stored on Defendant's system.

Plaintiff's Experiences

62. Plaintiff entrusted his Private Information to Defendant.

63. Prior to the Data Breach, Defendant retained Plaintiff's name, member ID, and information that Plaintiff provided during a health assessment.

64. Plaintiff provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

65. On July 27, 2022, Defendant notified Plaintiff that Defendant's network had been accessed and Plaintiff' Private Information may have been involved in the Data Breach.

66. Plaintiff is very careful about sharing sensitive Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

67. Plaintiff stores any documents containing his Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

68. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice

of Data Breach, as well as conducting self-monitoring of his accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

69. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

70. Plaintiff has also experienced a substantial increase in suspicious phone calls, emails, and text messages, which Plaintiff believes is related to his Private Information being placed in the hands of illicit actors.

71. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

72. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS ALLEGATIONS

73. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

74. The Nationwide Class that Plaintiff seek to represent is defined as follows:

> All United States residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice

> of Data Breach that Defendant published to Plaintiff and other Class Members on or around July 27, 2022 (the "Nationwide Class").

75. In addition, Plaintiff seeks to represent the following class of Minnesota residents as follows:

> All Minnesota residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach that Defendant published to Plaintiff and other Class Members on or around July 27, 2022 (the "Minnesota Class").

76. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

77. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

78. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds, if not thousands, of individuals whose PII may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.

79. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

80. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

81. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

82. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

83. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action

treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

84. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

85. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

86. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

87. Unless a Class-wide injunction is issued, Defendant may continue in their failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

88. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

89. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

90. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

91. Plaintiff and the Class entrusted Defendant with their Private Information.

92. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

93. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

94. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an

unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

95. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Classes in Defendant's possession was adequately secured and protected.

96. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII they were no longer required to retain pursuant to regulations.

97. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

98. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

99. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

100. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

101. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

102. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

103. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

104. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

105. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

106. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

107. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

108. Defendant, through their actions and/or omissions, unlawfully breached their duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care

in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

109. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

110. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

111. Defendant, through its actions and/or omissions, unlawfully breached their duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII.

112. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII they were no longer required to retain pursuant to regulations.

113. Defendant, through its actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

114. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

115. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Nationwide Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

116. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

117. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

118. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

119. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

120. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of those businesses' failure to use reasonable data security measures and avoid unfair and deceptive practices, caused identical harms to those suffered by Plaintiff and the Class.

121. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and

attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

122. As a direct and proximate result of Defendant' negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

123. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
Negligence *Per Se*
(On Behalf of Each Plaintiff and the Nationwide Class)

125. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

126. Pursuant to HIPAA and applicable federal and state law as set forth herein (*e.g.,* Wis. Stat. §§ 146.81, *et seq*.), Defendant had a duty to implement reasonable safeguards to protect Plaintiffs' and the Class Members' Private Information. Pursuant to applicable state laws as referred to herein, including but not limited to Wisconsin, Defendant had a duty to Plaintiffs and Class Members residing in those states to not disclose and to safeguard Plaintiffs' and Class Members' confidential Private Information.

127. In addition, pursuant to Wisconsin law (Wis. Stat. §§ 134.98(3)(a)), Defendant had a duty to provide notice to Plaintiffs and the Class Member within 45 days after it learned of the Data Breaches. Further, Defendant had a duty to notify "without unreasonable delay" all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 USC 1681a(p), of the timing, distribution, and content of the notices sent to the individuals. Wis. Stat. § 134.98(2)(br).

128. In addition to violations of HIPAA and state laws, Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits "unfair . . . practices in or affecting commerce" including, as recently interpreted by the Federal Trade Commission ("FTC"), acts or practices that fail to take reasonable measures to protect customers' personal information like the Private Information. Defendant violated Section 5 and similar statues by failing to employ reasonable security systems, controls and procedures to protect the PII of Plaintiffs and the other Class Members which violations constitutes negligence *per se*.

129. Defendant breached its duties under federal and state law to Plaintiff and the Class Members by providing access, exposing, and disclosing their information to third parties, by failing to safeguard and provide adequate security for their Private Information in an unreasonable manner, by failing to give timely notice to Plaintiffs and the Class Members, and by failing to the give the required information to national consumer reporting agencies without unreasonable delay. Defendant's failure to comply with these applicable laws and regulations constitutes negligence *per se*.

130. Plaintiff and the Class Members are the individuals the federal and state statues set forth herein seek to protect. For instance, the FTC Act expressly prohibits "unfair" acts that "cause or are likely to cause substantial injury to consumers which is not reasonably avoidable by consumers." Similarly, the other federal and state laws referred to herein seek to protect Plaintiffs and the Class Members.

131. Additionally, the harm that has occurred to Plaintiffs and the other Class Members is the type of harm the FTC Act and other federal and state laws set forth herein were intended to prevent and remedy. The FTC and other federal and state regulatory authorities have pursued a number of enforcement actions against businesses that caused the unauthorized dissemination, collection or use of their customers' Private Information and personal information as a result of the businesses' lack of reasonable and adequate security measures and practices.

132. But for Defendant's negligence *per se*, breach of their duties, and/or negligent supervision of their agents, contractors, vendors, and suppliers, Plaintiffs and the Class Members would not have suffered injury-in-fact. The injury and harm suffered by Plaintiffs and the Class Members was the reasonably foreseeable result of, and directly traceable to, Defendant's breach of its duties. Defendant knew or should have known that they were failing to meet their duties, and that

Defendant's breach thereof would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

133. As a direct, actual, and proximate result of Defendant's negligent conduct and/or negligence *per se*, Plaintiff and Class Members have been injured and are entitled to damages.

COUNT III
Unjust Enrichment
(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

134. Plaintiff and the Class repeat and re-allege each and every allegation in the Complaint as if fully set forth herein.

135. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

136. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff' and Class Members' PII.

137. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

138. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

139. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

140. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

141. Plaintiff and Class Members have no adequate remedy at law.

142. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

143. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

144. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
Invasion of Privacy
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

145. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

146. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

147. Defendant owed a duty to Plaintiff and Class Member to keep their Private Information confidential.

148. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiff' and Class Members' Private Information is highly offensive to a reasonable person.

149. Defendant's reckless and negligent failure to protect Plaintiff' and Class Members' Private Information constitutes an intentional interference with Plaintiff' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

150. Defendant's failure to protect Plaintiff' and Class Members' Private Information acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

151. Defendant knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

152. Because Defendant failed to properly safeguard Plaintiff's and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

153. As a proximate result of Defendant's acts and omissions, the private and sensitive Private Information of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

154. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

155. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiff and the Class.

156. Plaintiff, on behalf of himself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information.

157. Plaintiff, on behalf of himself and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT V
Breach of Confidentiality of Health Records, Wis. Stat. 146.81, *et seq*.
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

158. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

159. Wisconsin law regarding Confidentiality of Patient Health Care Records, Wis. Stat. §§ 146.81, *et seq*., states that:

> All patient health care records shall remain confidential. Patient health care records may be released only to the persons designated in this section or to other persons with the informed consent of the patient or of a person authorized by the patient." Wis. Stat. § 146.82(1).

160. The stolen Private Information belonging to Plaintiff and Class Members are "health care records" under Wis. Stat. § 146.81(4). [15]

161. Defendant violated Wis. Stat. §§ 146.81*, et seq*. when it compromised, allowed access to, released, and disclosed patient health care records and Private Information to third parties without the informed consent or authorization of Plaintiffs and Class Members. Defendant did not and does not have express or implied consent to disclose, allow access to, or release the Plaintiffs' and Members' Private Information. To the contrary, Defendant expressly undertook a duty and obligation to Plaintiffs and Class Members.

162. Defendant did not disclose to or warn the Plaintiffs and Class Members that their Private Information could be compromised, stolen, released, or disclosed to third parties without their consent as a result of Defendant's computer systems and software being outdated, easy to hack, inadequate, and insecure. Plaintiff and Class Members did not know or expect, or have any reason to know or suspect, that Defendant's computer systems and software were so outdated, easy to hack, inadequate, and insecure that it would expose their Private Information to unauthorized disclosure. In fact, they were told to the contrary in written statements and representations given to Plaintiff and Class Members, and on Defendant's website, namely that:

[15] "'Patient Health Care Records' means all records related to the health of a patient prepared by or under supervision of a health care provider;…" Wis. Stat. § 146.81(4).

> [Defendant] maintains commercially reasonable security measures to protect [Private Information] [Defendant] collects and store[s] from loss, misuse, destruction, or unauthorized access.[16]

163. Wis. Stat. § 146.84(1)(b) states:

> Any person, including the state or any political subdivision of the state, who violates Wis. Stat. § 146.82 or § 146.83 in a manner that is knowing and willful shall be liable to any person injured as a result of the violation for actual damages to that person, exemplary damages of not more than $25,000 and costs and reasonable attorneys' fees.

164. Wis. Stat. § 146.84(1)(b)(m) states:

> Any person, including the state or any political subdivision of the state, who negligently violates Wis. Stat. s. 146.82 or 146.83 shall be liable to *any person injured* as a result of the violation for actual damages to that person, *exemplary damages* of not more than $1,000 and costs and reasonable actual attorney fees." Wis. Stat. § 146.84(1)(bm). [*Emphasis added*.]

165. Wis. Stat. § 146.84(1)(c) states:

> "An individual may bring an action to enjoin any violation of s. 146.82 or 146.83 or to compel compliance with s. 146.82 or 146.83 and may, in the same action, seek damages as provided in this subsection."

166. Actual damages are not a prerequisite to liability for statutory or exemplary damages under Wis. Stat. § 146.81. A simple comparison of other Wisconsin statues (*e.g.*, Wis. Stat. § 134.97(3)(a) and (b), "Civil Liability; Disposal And Use" of records containing personal information), makes clear that the Wisconsin Legislature did not include an actual damages requirement in Wis. Stat. § 146.84 when it explicitly did so in other privacy statutes. *See* Wis. Stat. § 134.97(3)(a) and (b).

167. Similarly, the Wisconsin legislature made it clear that the exemplary damages referred to Wis. Stat. § 146.81 are not the same as punitive damages. Here, the plain language of

[16] https://1touchpoint.com/privacy-policy (last visited: August 3, 2022).

another Wisconsin statue (Wis. Stat. § 895.043(2), "Scope" of punitive damages), specifically and unequivocally excludes an award of "exemplary damages" under Wis. Stat. §§ 146.84(1)(b) and (bm) from the scope of "punitive damages" available under Section 895.043.[19] In short, exemplary damages under Wis. Stat. § 146.84(1)(b) and (bm) are not the same as either actual damages, or punitive damages; they are statutory damages available to persons who have been "injured" as a result of a negligent data breach like the one at issue here

168. The plain, common dictionary definition of "injure" is, " **injured**; **injuring** play \ˈinj-riŋ, ˈin-jə-\

transitive verb
1a : to do an injustice to **:** wrong
b : to harm, impair, or tarnish the standing of
- *injured* his reputation
c : to give pain to
- *injure* a person's pride
2a : to inflict bodily hurt on
b : to impair the soundness of
- *injured* her health
c : to inflict material damage or loss on."[17]

169. Plaintiff and Class Members request that the Court issue declaratory relief declaring Defendant's practice of using insecure, outdated, and inadequate email and computer systems and software that are easy to hack for storage and communication of Private Information data between Defendant and third parties unlawful. The Plaintiffs and Class Members further request the Court enter an injunction requiring Defendant to cease the unlawful practices described herein, and

[17] "Injure" Merriam Webster Online Dictionary (2021 ed.); *see also supra* note 5 (relying on Black's Online Law Dictionary (2d ed.) definition, stating an injury is "Any wrong or damage done to another, either In his person, rights, reputation, or property. Parker v. Griswold, 17 Conn. 298, 42 Am. Dec. 739; Woodruff v. Mining Co., 18 Fed. 781; Hitch v. Edgecombe County, 132 N. C. 573, 44 S. E. 30; Macauley v. Tierney, 19 R. I. 255, 33 Atl. 1, 37 L. R. A. 455, 61 Am. St. Rep. 770. In the civil law. A delict committed in contempt or outrage of anyone whereby his body, his dignity, or his reputation is maliciously injured. Voet, Com. Ad Pand. 47, t. 10, no. 1.

enjoining Defendant from disclosing or using Private Information without first adequately securing or encrypting it.

170. Plaintiff and Class Members request the Court order Defendant to identify, seek, obtain, encrypt, and retain at the conclusion of this action all existing Private Information in their possession or the possession of third parties and provide it to the Plaintiffs and Class Members.

171. Plaintiff and Class Members request that the Court enter an injunction ordering that Defendant:

a) engage a third-party ombudsman as well as internal compliance personnel to monitor, conduct test, and audit Defendant's safeguards and procedures on a periodic basis;
b) audit, test, and train its internal personnel regarding any new or modified safeguards and procedures;
c) conduct regular checks and tests on its safeguards and procedures;
d) periodically conduct internal training and education to inform internal personnel how to immediately identify violations when they occur and what to do in response;
e) meaningfully educate its former and current patients about their privacy rights by, without limitation, written statements describing with reasonable specificity the precautionary steps Defendant is taking to update its security technology to adequately secure and safeguard patient Private Information; and
f) identify to each Class Member in writing with reasonable specificity the Private Information of each such Class Member that was stolen in the Data Breach, including without limitation as required under Wis. Stat. § 134.98(3)(c).

172. Plaintiff and Class Members request the Court enter an Order pursuant to Wis. Stat. § 146.84(1)(bm) awarding minimum statutory exemplary damages of $1,000 to each Plaintiff and each Class Member whose Private Information was compromised and stolen, as well as attorneys' fees and costs.

COUNT VI
Wisconsin Deceptive Trade Practices Act, Wis. Stat. §§ 100.18, *et seq.*,
(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)

173. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

174. Defendant's conduct violates Wisconsin's Deceptive Trade Practices Act, Wis. Stat. §100.18 (the "WDTPA"),[23] which provides that no,

> "firm, corporation or association ... with intent to sell, distribute, increase the consumption of ... any ... merchandise ... directly or indirectly, to the public for sale ... shall make, publish, disseminate, circulate, or place before the public ... in this state, in a ... label ... or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public ... which ... contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

175. Plaintiff and Class Members "suffered pecuniary loss because of a violation" of the WDTPA. Wis. Stat. §100.18(11)(b)(2).

176. Defendant deliberated engaged in deceptive an unlawful practices on or around April 28, 2022 when Defendant continued to claim on its website that "We maintain commercially reasonable security measures to protect [Private Information] we collect and store from loss, misuse, destruction, or unauthorized access." Specifically, Defendant continued to make this claim even though Defendant knew its network had been accessed via the Data Breach.

177. Defendant further violated the WDTPA by: (a) fraudulently advertising material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; (b) misrepresenting material facts pertaining to its system and data services by representing and advertising that it would maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, so as to safeguard Private Information from unauthorized access; (c) omitting, suppressing, and concealing the material fact of the inadequacy of the security practices and procedures; (d) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain security practices and procedures to safeguard its systems and data from cyberattacks like the Data Breaches, to prevent infiltration of the security system so as to safeguard Private Information from unauthorized access; and (e) engaging in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the First Data Breach to enact reasonable security practices to safeguard its systems and data from cyberattacks like the Data Breaches.

178. The purpose of Defendant's misrepresentations set forth herein was to minimize the harm and injury-in-fact Plaintiffs and Class Members are facing caused by the Data Breach, and therefore increase the sales and use of Defendant's goods and services.

179. Defendant knew or should have known that its computer systems and security practices and procedures were inadequate and that risk of the Data Breaches and theft was high. Defendant’s actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and Class Members.

180. The Plaintiffs and the Class Members relied upon Defendant's deceptive and unlawful marketing practices and are entitled to damages, including reasonable attorney fees and costs, punitive damages, and other relief which the court deems proper. Wis. Stat. §§ 100.18(11)(b)(2) and 100.20(5).

COUNT VII
Violation of the Minnesota Health Records Act
Minn. Stat. § 144.291 and 144.293
(On Behalf of Plaintiff and the Putative Minnesota Rule 23 Class)

181. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

182. Under the Minnesota Health Records Act, "health record" means any information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to patient; or the past, present, or future payment for the provision of health care to a patient. Minn. Stat. § 144.291, subd. 2(c) (the "MHRA").

183. The Sensitive Information of Plaintiffs and the other Class members that was released in the Data Breach involved health records as that term is defined in the MHRA.

184. Plaintiffs and the other Class members are "patients" as that term is defined under the MHRA at all times relevant to this action under Minn. Stat. § 144.291, subd. 2(g).

185. Under the MHRA, it is unlawful for a third party to access a patient's health records from a provider, or a person who receives records from a provider, without the patient or the patient's legally authorized representative's consent, specific authorization in law, or a representative from a provider that holds a signed and dated consent from the patient authorizing the release. Minn. Stat. § 144.293, subd. 2(1-3).

186. Defendant released Plaintiffs' and the other Class members' health records.

187. Neither Plaintiffs nor the other Class members consented to have their health records released.

188. Under the MHRA, a provider or other person who causes an unauthorized release of a health record by negligently releasing the health record is liable to the patient for compensatory damages, plus costs and reasonable attorney fees. Minn. Stat. § 144.298, subd. 2. As a result of Defendant's violations of the MHRA, Plaintiffs and the other Class members are entitled to compensatory damages, plus costs and reasonable attorney fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected

through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demand that this matter be tried before a jury.

Date: August 3, 2022

Respectfully Submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

David K. Lietz
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave. NW, Ste. 440
Washington, D.C. 20015
Telephone: (866) 252-0878
dlietz@milberg.com

Bryan L. Bleichner
Philip J. Krzeski
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Counsel for Plaintiff and Putative Rule 23 Classes